Windows .NET Security

A Foundation for Trustworthy Computing

Dave Thompson

Vice President

Server Product Group

Microsoft Corporation

Microsoft Windows.net Server Family

Session Agenda

- Customer Challenges
- Microsoft Security Strategy
  - Secure Windows Initiative
  - Strategic Technology Protection Program
  - Trustworthy Computing
- Trustworthy Computing: Windows .NET and Secure Connected Infrastructure

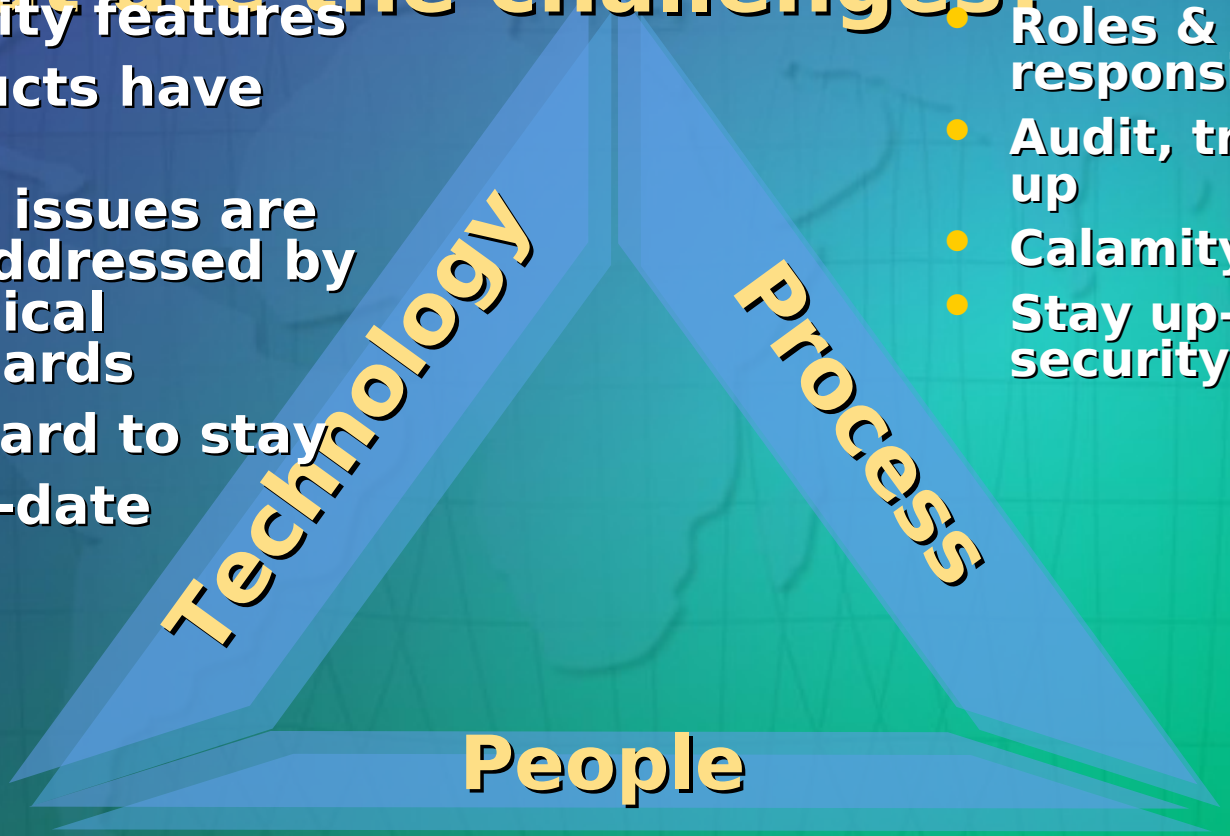
Microsoft's Commitment To Customers:

To do everything possible to enable every customer to work, communicate, and transact securely over the Internet

Technology, Process, People

What are the challenges?

- Products lack security features
- Products have bugs
- Many issues are not addressed by technical standards
- Too hard to stay up-to-date



- Design for security
- Roles & responsibilities
- Audit, track, follow-up
- Calamity plans
- Stay up-to-date with security developmen

People

- Lack of knowledge
- Lack of commitment
- Human error

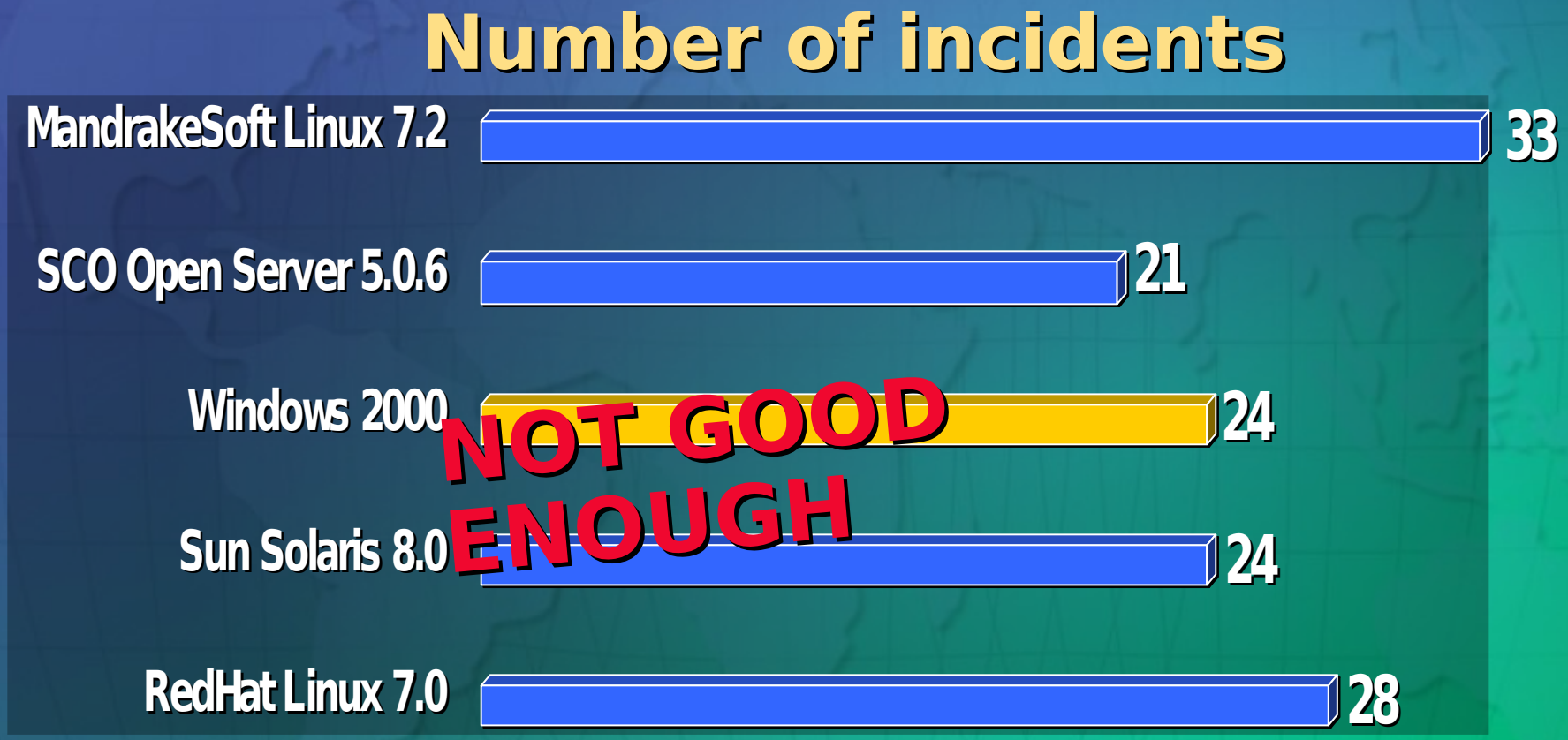
Microsoft Security Strategy

Secure Windows Initiative

"Engineering For Security"

Goal: Eliminate Every Security Vulnerability Before The Product Ships

Industry Yardstick



John McCormick, TechRepublic, Inc., September 24, 2001, based on data provided by Security Focus Bugtraq

Secure Windows Initiative

People

Train, and keep current, every developer, tester, and program manager in the specific techniques of building secure products

Process

Make security a critical factor in design, coding and testing of every product Microsoft builds

- Cross-group design & code reviews
- Security Threat Analysis part of every design spec
- Red Team testing and code reviews
- Focus *not* confined to buffer overruns
- Security bug feedback loop & code sign-off requirements
- External reviews and testing by consultants and public

Technology

Build tools to automate everything possible in the quest to code the most secure products

- Prefix and Prefast for buffer overrun detection
- Updated as new vulnerabilities found
- Visual C++ 7.0 compiler improvements
- Domain-specific tools (i.e. RPC security stress)

Secure Windows Initiative

External Security Review

- **FIPS 140-1 evaluation of Cryptographic Service Provider (CSP) – *Completed***
  - ***Government validation of base crypto algorithms in Windows***
- **Common Criteria evaluation – *In Preparation***
  - ***Evaluation of Windows source code against International security criteria for evaluating***
- **Third party expert review of key components**

Secure Windows Initiative

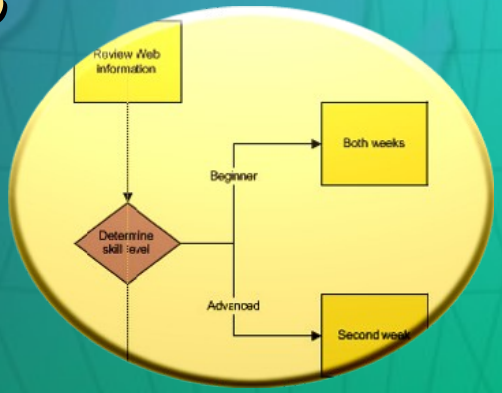
Breaking News…

- Windows Security Push
  - Mobilizing all contributors
  - Mandatory SWI training
  - Teams execute plans during February
  - Focus on all sources of vulnerability, reduction of attack surface, secure defaults and features
  - Identified vulnerabilities flagged for backport

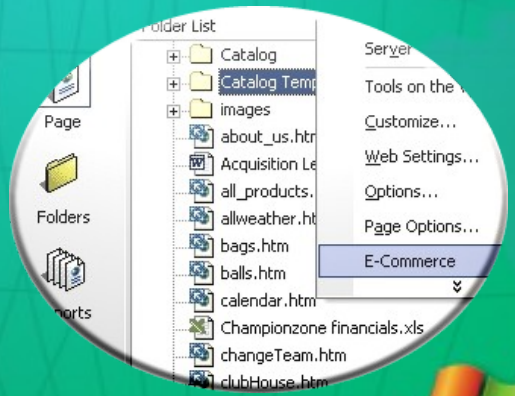
Strategic Technology Protection Program

Goal: Help customers secure their Windows Systems

People



Process



Technology

Windows.net Server Family

Strategic Technology Protection Program - Customers Need Our Help

More than 50% of the customers affected by Code Red were not patched in time for Nimda

- I didn’t know which patches I needed
- I didn’t know where to find the updates
- I didn’t know which machines to update
- We updated our production servers, but the rogue servers got infected

STPP: “Get Secure”

Now **- Free Virus Support Hotline (US & Canada)**

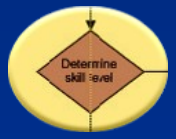
- **1-866-PCSAFETY (1-866-727-2338)**

Now **- Security Assessment Program Offering**

- **Available immediately through MCS/PSS**

Now **- Microsoft Security Toolkit**

- **Server oriented security resources for server admins**
- **New server security tools and updates, Windows Update bootstrap client for Windows 2000**



Coming **- Enterprise Security Tools**

- **Microsoft Baseline Security Analyzer**
- **SMS security patch rollout tool**
- **Windows Update Auto-update client**

Get Secure
Microsoft Security Toolkit

- Gets Windows NT and 2000 systems to secure baseline, even disconnected net
- Automates server updates
  - One-button wizard and SMS Scripts
- Updates and Patches
  - Includes ***all*** Service Packs and ***critical*** OS and IIS patches through 10/15
- HFNetchk: patch level verifier
- IIS Lockdown & URLScan

Microsoft Baseline Security Analyzer

demo

Michael Stephenson
Lead Product Manager
Windows Servers

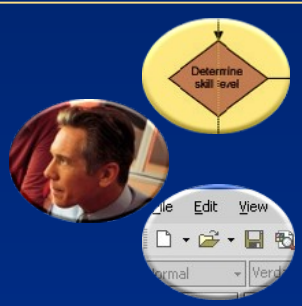
STPP: “Stay Secure”

Jan. 2002 **- Windows 2000 Security Rollup Patches**

- **Bundle all security fixes in single patches**
- **Reduces reboots and administrator burden**

Spring 2002 **- Windows 2000 Service Pack (SP3)**

- **Provide ability to install SP3 + security rollup with a single reboot**



Spring 2002 **- Federated Corporate Windows Update Program**

- **Allows enterprise to host and select Windows Update content**

Ongoing **- Enhanced Product Security**

- **Provide greater security enhancements in the releases of all new products, including the Windows .NET Server family**

Windows Update Corporate Edition

- For distribution of critical updates hosted on Windows update
- Delivers updates to auto-update clients
  - Only administrator approved updates
  - Basic logging
  - Web-based console
  - Will be integrated w/management products
- Auto-update client

Trustworthy Computing

Goal: Make devices powered by computers and software as trustworthy as devices powered by electricity.

A Trust Taxonomy

Goals

Availability
At advertised levels

Suitability
Features fit function

Integrity
Against data loss or alteration

Privacy
Access authorized by end-user

Reputation
System and provider brand

Means

Security
Resists unauthorized access

Quality
Performance criteria

Dev Practices
Methods, philosophy

Operations
Guidelines and benchmarks

Business Practices
Business model

Policies
Laws, regulations,

Execution

Intent
Management assertions

Risks
What undermines intent, causes liability

Implementation
Steps to deliver intent

Evidence
Audit mechanisms

What Trustworthy Computing Will Take

- What it will take:
  - Short-term: improved designs, implementation techniques, security policies
  - Medium term: new system management mechanisms and service strategies
  - Long-term: decade-long fundamental research and policy challenges

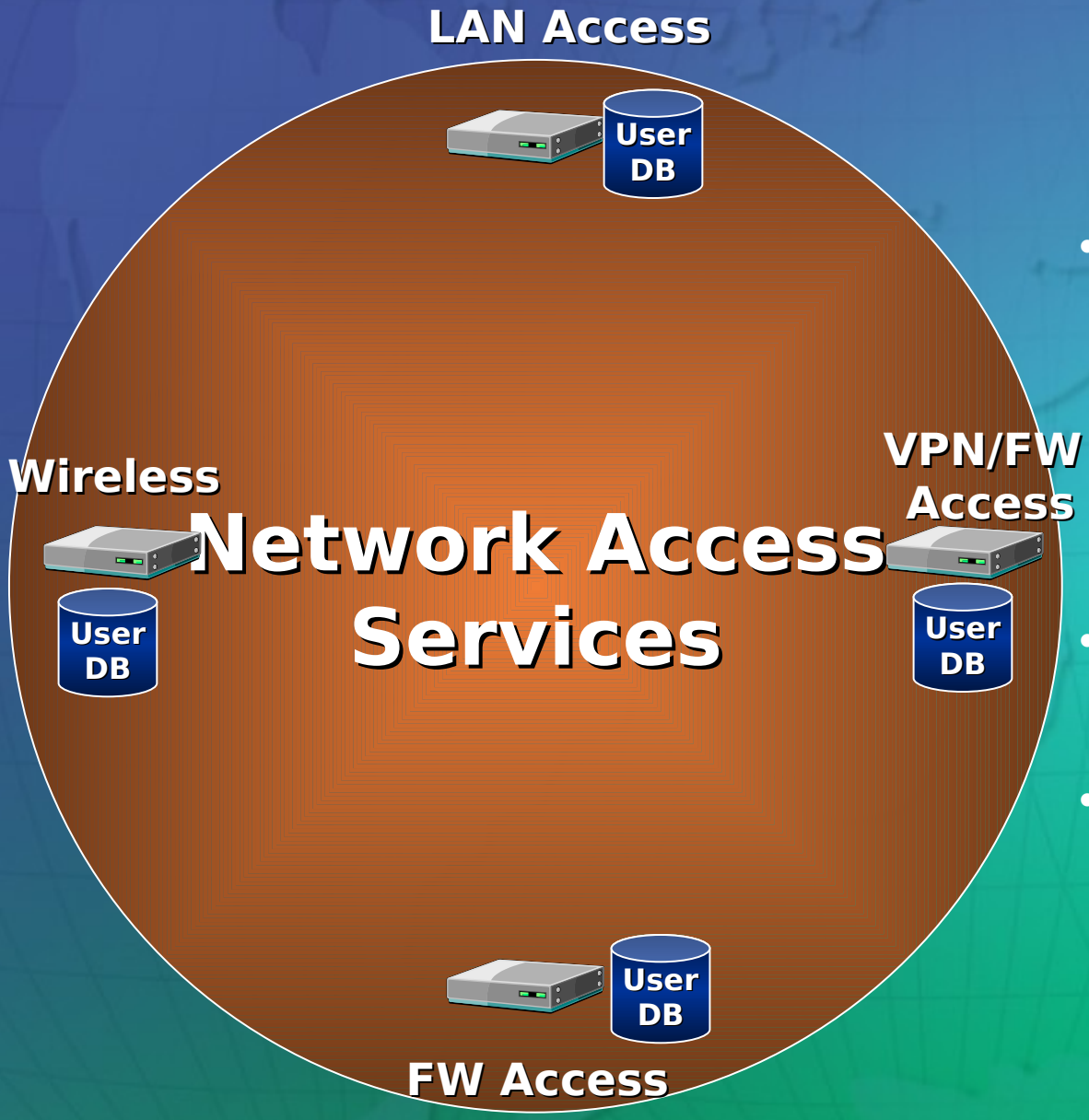
Trustworthy Computing:
Windows .NET and Secure Connected Infrastructure

Goal: Provide IT with a secure, integrated foundation for managing how users, business, and technologies connect.

Secure Connected Infrastructure

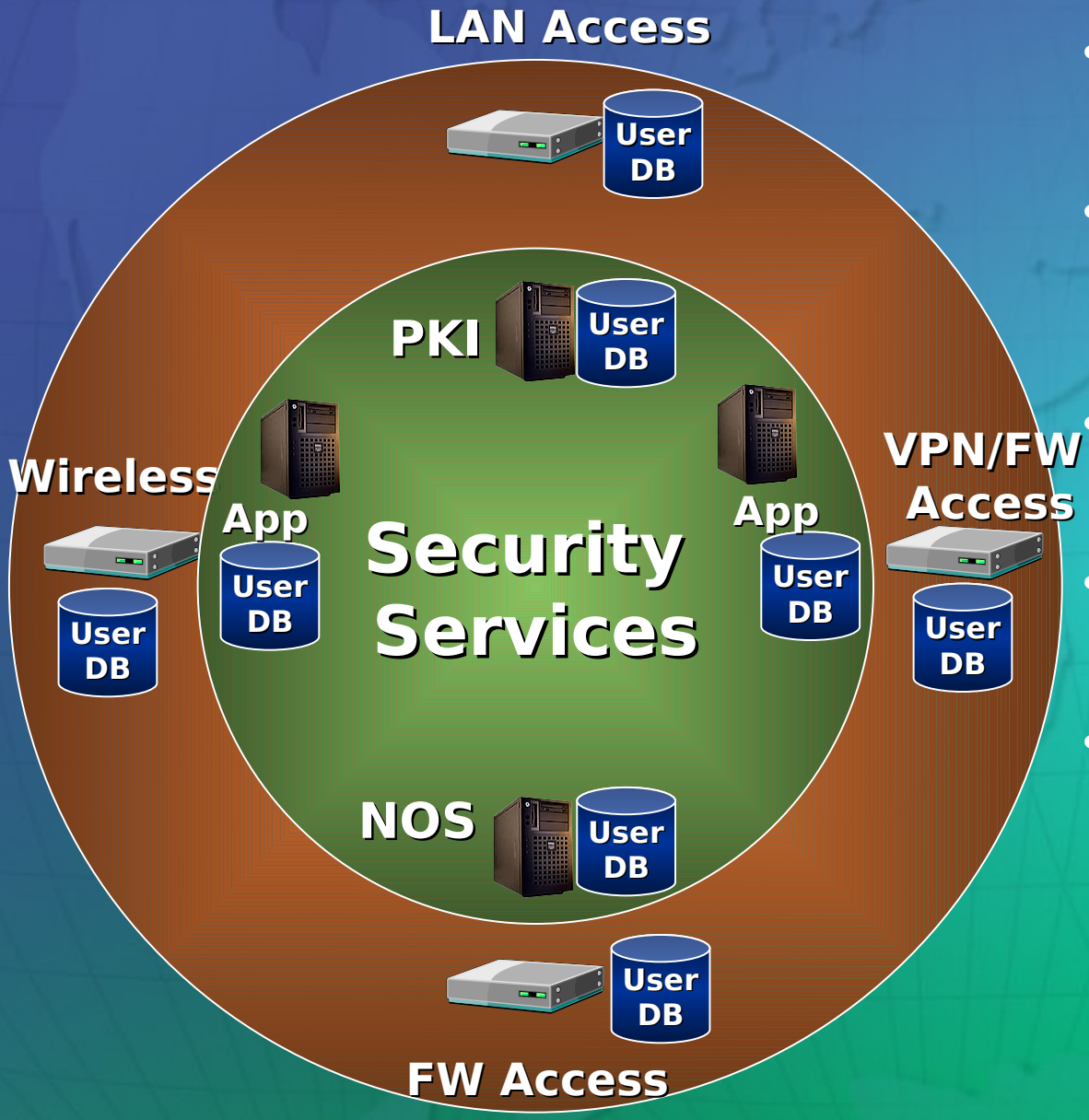
- **Secure** – End to end authentication and authorization from the client to the network gateway to the desired application or service.
- **Integrated** – A comprehensive set of infrastructure services designed to work together to provide customers with solutions that deliver the lowest TCO.
- **Connected** – Based on industry standards to enable IT to bring together employees, customers, business partners, and technology to increase automation and productivity.

Network Access Challenges



- Management of multiple secure network gateways
  - LAN
  - VPN
  - Firewall
  - Wireless
- Multiple identities for the same user
- How do I ensure only trusted users and computers access my network?

Secure Access Challenges



- Multiple authentication & authorization methods
- Applications can have their own set of identities
- PKI required for secure email, IPSEC, 802.1x …
- …PKI is difficult to deploy and manage
- How do I build an infrastructure that provides strong authentication and authorization across all my applications and services with single sign-on for my users?

Windows .NET Brings it Together

- Integrated network authentication and authorization
- Secure, authenticated wireless access via 802.1x support
- Authenticated firewall access via Microsoft ISA server
- Common store to manage identities
- Simplified PKI deployment and operations via the integrated PKI services and auto-enrollment
- Directory and identity synchronization across multiple directories via MMS
- Secure single sign-on from the client, to the network gateway, to the application.

Pocket Guide to Windows .NET Security

What you should be telling customers about Windows .NET Security

Windows .NET will be the Most *Secure* Microsoft Server OS	• **SWI: Engineering for security** • **STPP: Get secure and stay secure** • **Managed code reduces app vulnerabilities**
The *integration* of services in Windows .NET Simplifies Security	• **Unified directory and security** • **Strong authentication via PKI and Kerberos** • **Single-signon: client to network to application**
Windows .NET will be the best OS for secure *connected* IT Environments	• **Single model authenticated network access** • **Integrated firewall authentication w/ISA Server** • **Platform for federated authentication**

Microsoft's Commitment To Customers:

To do everything possible to enable every customer to work, communicate, and transact securely over the Internet

Questions?

Microsoft®